UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/443,204	11/18/1999	JOHN EDWARD FETKOVICH	EN998146	6903

30400 7590 12/14/2004

HESLIN ROTHENBERG FARLEY & MESITI P.C.
5 COLUMBIA CIRCLE
ALBANY, NY 12203

EXAMINER	
SANTOS, PATRICK J D	
ART UNIT	**PAPER NUMBER**
2161	

DATE MAILED: 12/14/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

COMMISSIONER FOR PATENTS
UNITED STATES PATENT AND TRADEMARK OFFICE
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450
www.uspto.gov

MAILED

[illegible] 2004

Technology Center 2100

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/443,204
Filing Date: November 18, 1999
Appellant(s): FETKOVICH ET AL.

For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed August 26, 2004.

(1) Real Party in Interest

A statement identifying the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The brief does not contain a statement identifying the related appeals and interferences which will directly affect or be directly affected by or have a bearing on the decision in the pending appeal is contained in the brief. Therefore, it is presumed that there are none. The Board, however, may exercise its discretion to require an explicit statement as to the existence of any related appeals and interferences.

(3) Status of Claims

The statement of the status of the claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Invention

The summary of invention contained in the brief is correct.

(6) Issues

The appellant's statement of the issues in the brief is correct.

(7) Grouping of Claims

The rejection of Claims 1, 2, 5, 7-14, 16-19, and 22-27 stand or fall together because appellant's brief does not include a statement that this grouping of claims does not stand or fall together and reasons in support thereof. See 37 CFR 1.192(c)(7).

The rejection of Claims 1, 13, 14, and 26 stand or fall together because appellant's brief does not include a statement that this grouping of claims does not stand or fall together and reasons in support thereof. See 37 CFR 1.192(c)(7).

The rejection of Claims 4 and 21 stand or fall together because appellant's brief does not include a statement that this grouping of claims does not stand or fall together and reasons in support thereof. See 37 CFR 1.192(c)(7).

The rejection of Claim 28 stands or falls together because appellant's brief does not include a statement that this grouping of claims does not stand or fall together and reasons in support thereof. See 37 CFR 1.192(c)(7).

The rejection of Claims 29, 32, and 34-38 stand or fall together because appellant's brief does not include a statement that this grouping of claims does not stand or fall together and reasons in support thereof. See 37 CFR 1.192(c)(7).

The rejection of Claim 31 stands or falls together because appellant's brief does not include a statement that this grouping of claims does not stand or fall together and reasons in support thereof. See 37 CFR 1.192(c)(7).

(8) Claims Appealed

The copy of the appealed claims contained in the Appendix to the brief is correct.

(9) Prior Art of Record

Examiner relies on the following prior art in the rejection of the claims under appeal:

5,412,730	Jones	05-1995
5,805,700	Nardone et al.	09-1998
5,933,501	Leppek	08-1999
5,991,403	Aucsmith et al.	11-1999
5,719,937	Warren et al.	02-1998

Chiariglione, Leonardo; "Digital Television Achieves Maturity"; copyrighted 1998, pp 2-3.

(10) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

- Claims 1, 2, 5, 7-14, 16-19, and 22-27 are rejected under 35 U.S.C. 103(a).
- Claims 1, 13, 14, and 26 are rejected under 35 U.S.C. 103(a).
- Claims 4 and 21 are rejected under 35 U.S.C. 103(a).
- Claim 28 is rejected under 35 U.S.C. 103(a).
- Claims 29, 32, and 34-38 are rejected under 35 U.S.C. 103(a).
- Claim 31 is rejected under 35 U.S.C. 103(a).

The above rejections are set forth in a prior Office Action, mailed on March 23, 2004. The prior Office Action is included below:

Claim Rejections - 35 USC § 112

1. Applicant's amendments to Claims 1, 3, 8, 11, 14, 24-25, 35, and 38 address the 35 USC §112, 2nd paragraph rejections of Claims 1-26, 35, and 38. Examiner withdraws the 35 USC §112, 2nd paragraph rejections of Claims 1-26, 35, and 38.

Claim Rejections - 35 USC § 103

2. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

3. Claims 1-3, 5-20, and 22-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,412,730 issued to Jones (Jones '730) in view of U.S. Patent No. 5,805,700 issued to Nardone et al. (Nardone '700) and in further view of U.S. Patent No. 5,933,501 issued to Leppek (Leppek '501).

<u>Claims 1, 2, 5-8, 12-19, and 26-27 (amended per response to applicant's arguments):</u>

Regarding Claim 1, Jones '730 teaches corresponding limitations, specifically a method for protecting a stream of data to be transferred between an encryption unit and a decryption unit (column 12, lines 25-27; Jones '730), said method comprising:

- encrypting the stream of data at a said encryption unit for transferring of said encrypted stream of data from said encryption unit to said decryption unit (column 12, lines 38-39; Jones '730);
- dynamically varying said encrypting of said stream of data at said encryption unit by changing at least one encryption parameter and signaling said change in encryption parameter to said decryption unit,

said dynamically varying of said at least one encryption parameter being responsive to occurrence of a predefined condition in said stream of data (column 12, lines 32-37 and column 12, lines 40-49; Jones '730); and

- decrypting said encrypted data at the decryption unit, said decrypting accounting for said dynamic varying of said encrypting by said encryption unit using said changed encryption parameter (column 12, lines 50-51; Jones '730).

The preferred embodiment of Jones '730 discloses an invention in which "means are employed at both the transmitting and receiving stations to monitor the flow of transmitted data and to advance the random number generator each time the transmitted data satisfies a predetermined condition" (column 1, lines 50-54; Jones '730). This advancement causes the change of the cryptographic key used to encrypt and decrypt the data stream, and thus constitutes dynamic variance.

Jones '730 does not teach the newly added limitation of "dynamically changing simultaneously multiple encryption parameters."

Nardone '700 teaches dynamically changing encryption parameters as described in paragraphs 12-13 below. However, Nardone '700 does not explicitly teach setting multiple parameters.

Leppek '501 teaches setting multiple parameters as described in paragraphs 12-13 below.

It would have been obvious to a person having ordinary skill in the art to combine Jones '730, Nardone 700, and Leppek '501 on the basis of the description in paragraphs 12-13 below.

Regarding Claim 2, Jones '730, Nardone '700, and Leppek '501 in combination teach corresponding limitations, specifically all the limitations of Claim 1 described above, plus specifying at least one encryption parameter that comprises "at least one of an encryption key, an encryption granularity, an encryption density scale, an encryption density, an encryption delay, an encryption key update variable, and an encryption key update data trigger" (column 12, lines 32-37 and column 12, lines 40-49; Jones '730). Jones '730 teaches the varying of the encryption key. Since this encryption key, which is varied, is one of the enumerated parameters, this constitutes varying at least one of the parameters enumerated in Claim 2. Furthermore, regarding Claim 2 as amended, Jones '730, Nardone '700, and Leppek '501 in combination address the issue of "multiple parameters" which also covers the issue of, "at least two parameters", as described in paragraphs 12-13 below.

Regarding Claim 5, Jones '730, Nardone '700, and Leppek '501 in combination teach corresponding limitations, specifically all the limitations of Claim 1 described above, plus specifying that "dynamically varying said encryption parameter based on passage of a predefined number of units of physical data or passage of a predefined number of conceptual units of data" (column 12, lines 35-37 and column 12, lines 48-49; Jones '730). Jones '730 teaches use of a block counter to measure the data stream in order to determine when to vary the cryptographic key used to encrypt and decrypt the

data stream (column 3, lines 33-36 and column 3, lines 64-68; Jones '730). Furthermore, regarding Claim 5 as amended, Jones '730, Nardone '700, and Leppek '501 in combination address the issue of "multiple parameters" as described in paragraphs 12-13 below.

Regarding Claim 6, Jones '730, Nardone '700, and Leppek '501 in combination teach corresponding limitations, specifically all the limitations of Claim 5 described above, plus specifying that the "encryption parameter comprises an encryption key" (column 8, lines 26-36; Jones '730).

Regarding Claim 7, Jones '730, Nardone '700, and Leppek '501 in combination teach corresponding limitations, specifically all the limitations of Claim 1 described above, plus specifying that the "stream of data comprises a stream a compressed data, and wherein said method further comprises decompressing said compressed data after said decrypting of said encrypted data by said decrypting unit" (column 2, line 29; column 8, line 5, and column 8, lines 16-22; Jones '730).

Regarding Claim 8, Jones '730, Nardone '700, and Leppek '501 in combination teach corresponding limitations, specifically all the limitations of Claim 7 described above, plus specifying that, "said stream of compressed data can comprise one of MPEG encoded video data, MPEG encoded audio data, and Dolby AC-3 audio data" (column 3, lines 12-16; Jones '730). In fact, the method of Jones '730 is independent of the format of the data to be transmitted. Furthermore, there are no non-obvious consequences of choosing to carry MPEG or AC-3 data. Regarding Claim 12, Jones '730, Nardone '700, and Leppek '501 in combination teach corresponding limitations, specifically all

the limitations of Claim 1 described above, plus specifying "said encrypting comprises encrypting multiple portions of said data stream and wherein said dynamically varying comprises dynamically varying said encrypting of said multiple portions of said data stream by changing said at least one encryption parameter for each portion of said multiple portions" (column 3, lines 19-25; Jones '730). Jones '730 explicitly teaches measuring the passage of data via a block counter and using a predetermined length as the criteria on when to change the encryption key. The length of bit stream delineated by the block counter constitutes a portion of the bit stream and varying the encryption key constitutes changing at least one encryption parameter. Furthermore, regarding Claim 12 as amended, Jones '730, Nardone '700, and Leppek '501 in combination address the issue of "multiple parameters" as described in paragraphs 12-13 below.

Regarding Claim 13, Jones '730 , Nardone '700, and Leppek '501 in combination teach corresponding limitations, specifically all the limitations of Claim 1 described above, plus specifying, "dynamically varying said at least one encryption parameter responsive to passage of a predefined number of data bits in said stream of data or alternatively, responsive to passage of a predefined number of data units in said stream of data wherein said data units comprise at least one of a program, a sequence, a group of pictures, a slice, or a macroblock" (column 3, lines 19-25; Jones '730). Jones '730 explicitly teaches measuring the passage of data via a block counter and using a predetermined length as the criteria on when to change the encryption key. Varying the encryption key constitutes changing at least one encryption parameter. Furthermore, Jones '730 states that, "Advantageously, the block counter may simply count the number

of bytes, words or blocks of data being transmitted ..." (column 3, lines 19-22; Jones '730). In the case of MPEG encoding, an implementer who wished to identify such an advantageous block of data would choose MPEG specific data lengths which include items such as a slice or a macroblock as enumerated in Claim 13. Furthermore, regarding Claim 13 as amended, Jones '730, Nardone '700, and Leppek '501 in combination address the issue of "multiple parameters" as described in paragraphs 12-13 below.

Regarding Claim 14, Jones '730, Nardone '700, and Leppek '501 in combination teach all the limitations of the claim using a similar argument as provided for Claim 1 above. Specifically, Jones '730 teaches a system that encrypts (column 12, lines 38-39; Jones '730) and decrypts (column 12, lines 50-51; Jones '730) data while varying an encryption parameter (column 12, lines 32-37 and column 12, lines 40-49; Jones '730). In the disclosed embodiment, the varying encryption parameter is an encryption key. Furthermore, regarding Claim 14 as amended, Jones '730, Nardone '700, and Leppek '501 in combination address the issue of "multiple parameters" as well as the issue of "simultaneous dynamic change", as described in paragraphs 12-13 below.

Regarding Claim 15, Jones '730, Nardone '700, and Leppek '501 in combination teach all the limitations of Claim 14 as described above. Furthermore, Jones '730 teaches varying of an encryption key (column 8, lines 26-36; Jones '730) using a similar argument as provided for Claim 6 above.

Regarding Claim 16, Jones '730, Nardone '700, and Leppek '501 in combination teach all the limitations of Claim 15 as described above. Furthermore, Jones '730 teaches the disclosed invention applied to digital data (column 3, lines 13-16; Jones '730).

Regarding Claim 17, Jones '730, Nardone '700, and Leppek '501 in combination teach all the limitations of Claim 14 as described above. Furthermore, Jones '730 teaches varying an encryption parameter according to the passage of bits (column 3, lines 16-25; Jones '730) using a similar argument as provided for Claim 5. Furthermore, regarding Claim 17 as amended, Jones '730, Nardone '700, and Leppek '501 in combination address the issue of "multiple parameters" as described in paragraphs 12-13 below.

Regarding Claim 18, Jones '730, Nardone '700, and Leppek '501 in combination teach all the limitations of Claim 17 as described above. Furthermore, Jones '730 teaches encrypting multiple portions of a bit stream (column 3, lines 19-25; Jones '730) using similar argument as provided for Claim 12 above. Furthermore, regarding Claim 18 as amended, Jones '730, Nardone '700, and Leppek '501 in combination address the issue of "multiple parameters" as described in paragraphs 12-13 below.

Regarding Claim 19 Jones '730, Nardone '700, and Leppek '501 in combination teach all the limitations of Claim 14 as described above. Furthermore, Jones '730 teaches varying at least one encryption parameter (column 12, lines 32-37 and column 12, lines 40-49; Jones '730) using a similar argument as provided for Claim 2 above. Furthermore, regarding Claim 19 as amended, Jones '730, Nardone '700, and Leppek '501 in combination address the issue of "multiple parameters" as described in paragraphs 12-13 below.

Regarding Claim 26, Jones '730, Nardone '700, and Leppek '501 in combination teach all the limitations of Claim 14 as described above. Furthermore, Jones '730 teaches the additional limitation of Claim 26, that an encryption parameter be varied for a block

of data (column 3, lines 19-25; Jones '730) using a similar argument as provided for Claim 13 above. Furthermore, regarding Claim 26 as amended, Jones '730, Nardone '700, and Leppek '501 in combination address the issue of "multiple parameters" as described in paragraphs 12-13 below.

Regarding Claim 27, Jones '730, Nardone '700, and Leppek '501 in combination teach corresponding limitations, specifically a system for protecting a stream of data to be transferred between a sender and a receiver (column 1, lines 37-42; Jones '730), said system comprising:

- an encryption unit disposed at said sender for encrypting the stream of data prior to transfer to said receiver, said encryption unit being adapted to dynamically vary encrypting of the stream of data by changing at least one encryption parameter based on an occurrence of a predefined condition in said data stream and signaling said change in encryption parameter to said receiver (column 12, lines 38-39; column 12, lines 32-37; and column 12, lines 40-49; Jones '730); and
- a decryption unit disposed at said receiver for decrypting said encrypted data, said decryption unit being adapted to receive said changed encryption parameter to account for said dynamic varying of said encrypting by said encryption unit using said changed encryption parameter (column 12, lines 50-51; Jones '730).

The preferred embodiment of Jones '730 discloses an invention in which "means are employed at both the transmitting and receiving stations to monitor the flow of

transmitted data and to advance the random number generator each time the transmitted data satisfies a predetermined condition" (column 1, lines 50-54; Jones '730). This advancement causes the change of the cryptographic key used to encrypt and decrypt the data stream, and thus constitutes dynamic variance of at least one encryption parameter.

Furthermore, regarding Claim 27 as amended, Jones '730, Nardone '700, and Leppek '501 in combination address the issue of "multiple parameters" and "dynamically changing parameters simultaneously" as described in paragraphs 12-13 below.

Claims 3, 9-11, 20, and 22-25 (as amended):

Regarding Claim 3, Jones '730 teaches all the limitations of Claim 2 as described above. Jones '730 does not teach varying the following multiple encryption parameters: "an encryption key, an encryption granularity, an encryption density scale, an encryption density, an encryption delay, an encryption key update variable, and an encryption key update data trigger" simultaneously, and furthermore only explicitly teaches varying the encryption key, update variable, and trigger.

Nardone '700, explicitly teaches encrypting a bit stream taking into account encryption granularity, density, and delay (column 3, line 65 to column 4, line 13; Nardone '700). Furthermore, Nardone '700 teaches selectively encrypting a bit stream rather than encrypting the entire bit stream (column 3, line 65 to column 4 line 13; Nardone '700). Nardone '700 does not explicitly teach combining with other encryption algorithms.

Leppek '501 teaches varying arbitrary encryption schemes in order to encrypt a bit stream.

To incorporate the variance of encryption key data as taught by Jones '730, the encryption granularity and density data as taught by Nardone '700, in addition to any other arbitrary encryption scheme, using the method taught by Leppek '501, would have been obvious to a person having ordinary skill in the art at the time of the invention as the combination of the same is necessary and explicitly taught therein as will be demonstrated below.

The motivation to vary encryption schemes on a bit stream and not just to use the Jones '730 encryption key variance method, is suggested by Leppek '501 teaching that "a fundamental characteristic of essentially all encryption operators or algorithms is the fact that, given enough resources, almost any encryption algorithm can be broken. This, coupled with the fact that each encryption algorithm has a 'footprint', which is discernable in the scrambled data by a sophisticated data communications analyst, means that no data communication can be guaranteed as secure" (column 1, lines 54-60; Leppek '501). In other words, using the same encryption scheme on a continuous bit stream will eventually provide a statistically significant amount of data for a hacker to break the encryption scheme. Thus Leppek '501 discloses an invention that, "combines selected ones of plurality of different encryption operators" (column 1, lines 65-67; Leppek '501). Furthermore he goes on to teach, "The encryption routines ... need not be any particular type of encryption algorithm, and may be conventional encrypting operators, such as PGP, DES..." (column 4, lines 13-17; Leppek '501). Thus Leppek '501 teaches necessity for an implementer using the Jones '730 encryption key variance method, to vary the encryption scheme itself in order to reduce the cryptographic footprint of the bit stream.

The motivation to choose the Nardone '700 granularity/density/delay variance method as an additional encrypting scheme required by the Jones '730/Leppek '501 combination is suggested by Nardone '700 teaching, "Experience has shown that the decryption and decompression of a fully encrypted MPEG compressed movie can consume as much as 30% of the available processor cycles, even with the latest high performance processors" (column 1, lines 32-38; Nardone '700). An implementer who wished to apply the Jones '730/Leppek '501 combination to MPEG data in order to take advantage of the MPEG market, would be motivated to choose an encryption algorithm that was not computationally intensive. In fact, Nardone '700 goes on to teach an approach, in which, "a fraction of the BTUs (Basic Transfer Units) ... are encrypted ...; only a few percent of the processor cycles required by the total encryption approach for decryption will be required to decrypt and render the {CVD+} (the encrypted bit stream)..." (column 3, line 65 to column 4 line 13; Nardone '700). Thus, Nardone '700 teaches the necessity for an implementer using the Jones '730/Leppek '501 combination to use the Nardone '700 granularity/density/delay variance method as an alternate for the Jones '730 encryption key variance method.

The motivation to use the Nardone '700 granularity/density/delay variance method with the Jones '730 encryption key variance method in combination, in the context of reducing cryptographic footprint as taught by Leppek '501 is also suggested by the Nardone '700 teaching to selectively encrypt the bit stream. As described above. Nardone '700 teaches that one can approximate bit stream degradation achieved by total encryption, by partially encrypting the bit stream, and one would further achieve the

benefit of requiring less processor cycles. Thus an implementer would be motivated to use the Jones '730 encryption key variance method to selectively encrypt the bit stream rather than the entire bit stream as taught by Nardone '700. Thus Nardone '700 teaches the necessity for an implementer using the Jones '730/Leppek '501 combination to use the Nardone '700 granularity/density/delay variance method not only as an alternate for the Jones '730 encryption key variance method but also in conjunction with each other.

In summary, since it would have been necessary for an implementer using the Jones '730 encryption key variance method to reduce cryptographic footprint by using the method of Leppek '501; and since it would have been necessary for an implementer to choose a low processing overhead encryption method such as the Nardone '700 granularity/density/delay scheme as an alternate encryption algorithm in order to efficiently encrypt multimedia data; and since furthermore it would have been necessary to use the Nardone '700 granularity/density/delay scheme in conjunction with the Jones '730 encryption key variance method in order to have the Jones '730 method itself be efficient for encrypting multimedia data; it would have been necessary and obvious to a person having ordinary skill in the art to combine the teachings of Jones '730, Nardone '700, and Leppek '501 as described above. Thus Claim 3 is rejected under 35 USC 103(a).

Regarding Claim 9, Jones '730 teaches all the limitations of Claim 1 as described above, including the varying of an encryption key. However, Jones '730 does not teach a "plurality of encryption parameters being employed by said encrypting and wherein said changed encryption parameter of said dynamically varying comprises one encryption

parameter of said plurality of encryption parameters." Furthermore, Jones '730 does not teach "initializing a plurality of encryption parameters based on sensitivity of said stream of data."

Leppek '501 teaches the use of multiple encryption algorithms as described above. Leppek '501 also teaches "initializing a plurality of encryption parameters" (column 4, lines 52-66; Leppek '501) but does not use sensitivity of the bit stream as a criterion for initialization.

Nardone '700 teaches the varying of granularity and density encryption, specifically only encrypting a selected portion of a bit stream as described above. Nardone '700 also teaches "sensitivity of said stream of data" as a criterion for encryption parameter initialization (column 3, line 65 to column 4 line 13; Nardone '700).

To incorporate the variance of encryption key data as taught by Jones '730, the encryption granularity and density data as taught by Nardone '700, in addition to any other arbitrary encryption scheme, using the method taught by Leppek '501, would have been obvious to a person having ordinary skill in the art at the time of the invention as the combination of the same is necessary and explicitly taught therein as described above. Furthermore, it would have been obvious and necessary to a person having ordinary skill in the art at the time of the invention by the applicant to combine the to initialize the plurality of parameters as taught by Leppek '501, based on the sensitivity of the bitstream as taught by Nardone '700 as will be demonstrated below.

The motivation to combine the Jones '730 / Nardone '700 / Leppek '501 in order to provide for "plurality of encryption parameters being employed by said encrypting and wherein said changed encryption parameter of said dynamically varying comprises one encryption parameter of said plurality of encryption parameters" is the same motivation as described in Claim 3.

The motivation to combine the "initializing a plurality of encryption parameters based on sensitivity of said stream of data" as taught by Leppek '501 into the Jones '730 / Nardone '700 / Leppek '501 combination is suggested by the fact that the Leppek '501 scheme delegates actual encryption to other algorithms and these algorithms inherently require initialization. Leppek '501 describes his disclosed invention as a "virtual encryption scheme" in which "the overall encryption operator itself does not actually perform any encrypting of the data. Instead, it assembles selected ones of a plurality of true encryption mechanisms into a cascaded sequence ..." (column 2, lines 6-13; Leppek '501). Thus the Leppek '501 invention would have to delegate to other encryption methods in order to actually encrypt the bit stream. Both the Jones '730 and Nardone '700, which are used in combination with Leppek '501 require initialization choices to be made (column 3; lines 26-40; Jones '730 and column 1, lines 50-59; Nardone '700). Thus in order to be used in combination with the invention of Leppek '501, the Jones '730 and Nardone '700 algorithms must be initialized. Furthermore, Nardone '700 teaches a motivation to set encryption granularity and density in order to reduce processing cycles (column 3, line 65 to column 4 line 13; Nardone '700). From this it is inherent that the initialization values should be set based on a tradeoff between

processing overhead and adequate encryption. Thus it would have been obvious to a person having ordinary skill in the art at the time of the invention by the applicant to combine the to initialize the plurality of parameters as taught by Leppek '501, based on the sensitivity of the bitstream as taught by Nardone '700.

Furthermore, regarding Claim 9 as amended, Jones '730, Nardone '700, and Leppek '501 in combination address the issue of "multiple parameters" as described in paragraphs 12-13 below.

Regarding Claim 10, Jones '730 teaches all the limitations of Claim 1 as described above. Jones '730 does not explicitly teach the setting and varying of parameters, nor does it explicitly teach the use of MPEG compressed data as the data payload of a bit stream, nor does it explicitly teach the use of sensitivity of the bit stream for a criterion for setting parameters.

Leppek '501 teaches the use of multiple encryption algorithms as described above. Leppek '501 also teaches "setting a plurality of encryption parameters" (column 4, lines 52-66; Leppek '501) but does not use sensitivity of the bit stream as a criterion for initialization.

Nardone '700 teaches the varying of granularity and density encryption, specifically only encrypting a selected portion of a bit stream as described above. Nardone '700 also teaches "sensitivity of said stream of data" as a criterion for encryption parameter initialization (column 3, line 65 to column 4 line 13; Nardone '700). Moreover, Nardone '700 teaches an embodiment in which the bit stream is

composed of MPEG compliant video data and MPEG compliant audio data including Dolby AC-3 data (column 2, lines 56-66; Nardone '700).

The motivation to combine the Jones '730 / Nardone '700 / Leppek '501 in order to provide for "plurality of encryption parameters for use by said encrypting" is the same motivation as described in Claim 3.

The motivation to use MPEG compressed data as the payload of the Jones '730 / Nardone '700 / Leppek '501 in combination would be to make the combination applicable to the large MPEG market. A practitioner would have been motivated to use MPEG compliant data as the payload in the Jones '730 / Nardone '700 / Leppek '501 combination. In fact, the motivation to use the Nardone '700 granularity/density/delay encryption method was motivated by balancing processing overhead with encryption security in multimedia data.

The motivation to use sensitivity of stream data as a criterion for encryption parameter initialization in the Jones '730 / Nardone '700 / Leppek '501 combination is the same motivation as described in Claim 9.

Thus, it would have been necessary and obvious to a person having ordinary skill in the art to use MPEG compressed data and to use sensitivity of stream data as a criterion for encryption parameter initialization in the Jones '730 / Nardone '700 / Leppek '501 combination.

Furthermore, regarding Claim 10 as amended, Jones '730, Nardone '700, and Leppek '501 in combination address the issue of "multiple parameters" as described in paragraphs 12-13 below.

Regarding Claim 11, Jones '730 teaches the limitations of Claim 1 as described above. Jones '730 does not teach all the limitations of Claim 10. Furthermore, Jones '730 does not teach the setting of a, "plurality of encryption parameters ... establishing at least some of an encryption granularity, and initial encryption key, a density scale, a density, an encryption delay, and a key update data trigger for said stream of MPEG encoded data."

Leppek '501 teaches the use of multiple encryption algorithms as described above. Leppek '501 also teaches "setting a plurality of encryption parameters" (column 4, lines 52-66; Leppek '501) but does not use sensitivity of the bit stream as a criterion for initialization.

Nardone '700 teaches the varying of granularity and density encryption, specifically only encrypting a selected portion of a bit stream as described above. Nardone '700 also teaches "sensitivity of said stream of data" as a criterion for encryption parameter initialization (column 3, line 65 to column 4 line 13; Nardone '700). Moreover, Nardone '700 teaches an embodiment in which the bit stream is composed of MPEG compliant video data and MPEG compliant audio data including Dolby AC-3 data (column 2, lines 56-66; Nardone '700).

The motivation to combine Jones '730 / Nardone '700 / Leppek '501 in order to provide for the setting of "plurality of encryption parameters ... establishing at least some of an encryption granularity, and initial encryption key, a density scale, a density, an encryption delay, and a key update data trigger," is described in the discussion regarding Claim 10 above.

The motivation to apply the Jones '730 / Nardone '700 / Leppek '501 combination method to a "stream of MPEG encoded data" is described in the discussion regarding Claim 3 above.

As such it would have been necessary and obvious to a person having ordinary skill in the art apply the setting of the enumerated encryption parameters to MPEG encoded data.

Furthermore, regarding Claim 11 as amended, Jones '730, Nardone '700, and Leppek '501 in combination address the issue of "multiple parameters" as described in paragraphs 12-13 below.

Regarding Claim 20, Jones '730 teaches all the limitations of Claim 19 as described above. Jones '730 does not teach the setting multiple encryption parameters, including in combination.

Nardone '700 teaches the setting of a encryption granularity/density/delay and the selective encoding of a bit stream as described above.

Leppek '501 teaches the rotating among several encryption algorithms as described above.

The motivation to combine Jones '730 / Nardone '700 / Leppek '501 to set multiple encryption parameters is the same as described in the discussion regarding Claim 3. As such, it would have been necessary and obvious for a person having ordinary skill in the art to modify Jones '730 to set multiple encryption parameters, including in combination, as described in the discussion above regarding Claim 3. Thus Claim 20 is rejected under 35 USC 103(a).

Regarding Claim 22, Jones '730 teaches all the limitations of Claim 14 as described above. However, Jones '730 does not teach setting of multiple parameters based on sensitivity of the data.

Nardone '700 teaches the setting of a encryption granularity/density/delay and the selective encoding of a bit stream as described above. Nardone '700 also teaches "sensitivity of said stream of data" as a criterion for encryption parameter initialization as described above.

Leppek '501 teaches the rotating among several encryption algorithms as described above.

The motivation combine Jones '730, Nardone '700, and Leppek '501 in order to set of multiple parameters based on sensitivity of the data is described in the discussion above regarding Claim 9. As such, it would have been necessary and obvious for a person having ordinary skill in the art to modify Jones '730 to set multiple parameters based on sensitivity of data. Thus Claim 22 is rejected under 35 USC 103(a).

Regarding Claim 23, Jones '730 teaches all the limitations of Claim 14 as described above. Jones '730 does not explicitly teach the additional limitations of Claim 22 which Claim 23 incorporates. Furthermore, Jones '730 does not explicitly teach the use of a decompression decoder.

Nardone '700 teaches the setting of a encryption granularity/density/delay and the selective encoding of a bit stream as described above. Nardone '700 also teaches "sensitivity of said stream of data" as a criterion for encryption parameter initialization as described above. Furthermore, Nardone '700 explicitly teaches the use of compressed

MPEG data (column 2, lines 56-66; Nardone '700), which implies an MPEG decoder, which in turn implies a decompression decoder.

Leppek '501 teaches the rotating among several encryption algorithms as described above.

The motivation to combine Jones '730 with Nardone '700 and Leppek '501, to set a plurality of encryption parameters is described in the discussion above regarding Claim 22.

The motivation to combine Jones '730 with Nardone '700 and Leppek '501 in order to carry compressed data and to use MPEG data is inherent in the the desire to carry MPEG data. In fact, Nardone '700 explicitly teaches the use of MPEG data. As a result, in order to render the data, adding an MPEG decoder after encryption is inherent in the Jones '730 / Nardone '700 / Leppek '501 combination. Since MPEG is inherently a compression standard, addition of the MPEG decoder constitutes adding a decompression decoder. As such, it would have also been necessary and obvious for a person having ordinary skill in the art to combine Jones '730 with Nardone '700 and Leppek '501 not only for the reasons enumerated in the discussion regarding Claim 22, but also for the benefit of a decompression decoder. Thus Claim 23 is rejected under 35 USC 103(a).

Regarding Claim 24, Jones '730 teaches all the limitations of Claim 14 above. However, Jones '730 does not explicitly teach all the limitations of Claim 23 which Claim 24 incorporates. Furthermore, Jones '730 does not explicitly teach the use of MPEG, video and audio, and Dolby AC-3 data for the data payload.

Nardone '700 teaches the setting of a encryption granularity/density/delay and the selective encoding of a bit stream as described above. Nardone '700 also teaches "sensitivity of said stream of data" as a criterion for encryption parameter initialization as described above. Furthermore, Nardone '700 explicitly teaches the use of compressed MPEG data (column 2, lines 56-66; Nardone '700), which implies an MPEG decoder.

Leppek '501 teaches the rotating among several encryption algorithms as described above.

The motivation to combine Jones '730 / Nardone '700 / Leppek '501 to set a plurality of encryption parameters and to use compressed data is described in the discussion regarding Claim 23 above.

The motivation to combine Jones '730 / Nardone '700 / Leppek '501 to use MPEG data is inherent in the discussion regarding Claim 23 above. The counterexample in the discussion above on Claim 23 explicitly refers to the Nardone '700 in which MPEG, video and audio, and Dolby AC-3 data is used for the data payload (column 2, lines 56-66; Nardone '700). Thus it would have been obvious for a person having ordinary skill in the art to combine Jones '730 / Nardone '700 / Leppek '501 in order to set multiple encryption parameters, and to use MPEG/AC-3 multimedia data for a data payload. Thus Claim 24 is rejected under 35 USC 103(a).

Regarding Claim 25, Jones '730 teaches all the limitation of Claim 14 above. However, Jones '730 does not explicitly teach all the limitations of Claim 23 which Claim 25 incorporates. Furthermore, Jones '730 does not explicitly teach the limitation of initializing a number of encryption parameters.

Nardone '700 teaches the setting of a encryption granularity/density/delay and the selective encoding of a bit stream as described above. Nardone '700 also teaches "sensitivity of said stream of data" as a criterion for encryption parameter initialization as described above. Furthermore, Nardone '700 explicitly teaches the use of compressed MPEG data (column 2, lines 56-66; Nardone '700), which implies an MPEG decoder.

Leppek '501 teaches the rotating among several encryption algorithms as described above. Leppek '501 also teaches the initialization of encryption parameters as described above.

The motivation to combine Jones '730 / Nardone '700 / Leppek '501 in order to meet the limitations of Claim 23 is described in the above discussion regarding Claim 23.

The motivation to combine Jones '730 / Nardone '700 / Leppek '501 in order to meet initialize multiple encryption parameters is described in the above discussion regarding Claim 11.

Thus it would have been obvious for a person having ordinary skill in the art to combine Jones '730 / Nardone '700 / Leppek '501 to meet the limitations of Claim 25. Thus Claim 25 is rejected under 35 USC 103(a).

4. Claims 1, 13, 14, and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over by U.S. Patent No. 5,991,403 issued to Aucsmith et al. (Aucsmith '403), in view of Nardone '700, and Leppek '501.

<u>Claims 1 and 13 (as amended):</u>

Regarding Claims 1 and 13, Aucsmith '403 teaches corresponding limitations, specifically all the limitations of Claim 1: encrypting data (column 4, lines 55-65; Aucsmith '403), varying an encryption parameter (column 2, lines 28-30; Aucsmith '403), and decrypting the data (column 4, line 66 to column 5, line 8; Aucsmith '403). Furthermore it specifies the additional limitation of Claim 13: "dynamically varying said at least one encryption parameter responsive to passage of a predefined number of data bits in said stream of data or alternatively, responsive to passage of a predefined number of data units in said stream of data wherein said data units comprise at least one of a program, a sequence, a group of pictures, a slice, or a macroblock" (column 2, lines 28-30; Aucsmith '403).

In the preferred embodiment, the parameter being varied is an encryption key and the data unit to be encrypted is a group of pictures (GOP) (column 2, lines 28-30; Aucsmith '403).

Furthermore, regarding Claims 1 and 13 as amended, Aucsmith '403 teaches corresponding limitations as Jones '730. However, Aucsmith '403 does not explicitly teach the additional limitations regarding "dynamically changing parameters simultaneously" and "multiple parameters."

Nardone '700 teaches dynamically changing encryption parameters as described in paragraphs 12-13 below. However, Nardone '700 does not explicitly teach setting multiple parameters.

Leppek '501 teaches setting multiple parameters as described in paragraphs 12-13 below.

It would have been obvious to a person having ordinary skill in the art to combine Aucsmith '403, Nardone 700, and Leppek '501 on the same basis as described in paragraphs 12-13 below wherein the Jones '730 reference is replaced with the Aucsmith '403 reference.

Claims 14 and 26 (as amended):

Regarding Claims 14 and 26, Aucsmith '403 teaches corresponding limitations, specifically all the limitations of Claim 14: varying an encryption parameter (column 2, lines 28-30; Aucsmith '403), and decrypting the data (column 4, line 66 to column 5, line 8; Aucsmith '403). Aucsmith '403 also teaches the additional limitation of Claim 26 on the same basis as described in the discussion on Claim 13 above: the varying parameter is an encryption key and the data unit is a GOP (column 2, lines 28-30; Aucsmith '403).

Furthermore, regarding Claims 14 and 26 as amended, Aucsmith '403 teaches corresponding limitations as Jones '730. However, Aucsmith '403 does not explicitly teach the additional limitations regarding "dynamically changing parameters simultaneously" and "multiple parameters."

Nardone '700 teaches dynamically changing encryption parameters as described in paragraphs 12-13 below. However, Nardone '700 does not explicitly teach setting multiple parameters.

Leppek '501 teaches setting multiple parameters as described in paragraphs 12-13 below.

It would have been obvious to a person having ordinary skill in the art to combine Aucsmith '403, Nardone 700, and Leppek '501 on the same basis as described in

paragraphs 12-13 below wherein the Jones '730 reference is replaced with the Aucsmith '403 reference.

5. Claims 4 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jones '730 in view of Nardone '700 and Leppek '501 and in further view of "Digital Television Achieves Maturity" by Leonardo Chiariglione, copyrighted 1998 (Chiariglione '98).

Claim 4:

Regarding Claim 4, Jones '730 / Nardone '700 / Leppek '501 in combination teach all the limitations of Claim 3 as described above. Furthermore, Nardone '700 teaches varying encryption schemes via a policy (column 2, lines 40-46; Nardone '700) and furthermore in a disclosed embodiment teaches varying the policy dynamically (column 4, lines 23-42; Nardone '700). However, Jones '730 / Nardone '700 / Leppek '501 do not teach multiplexing in the variance information into the encrypted bit stream.

Chiariglione '98 teaches multiplexing in the variance information into the encrypted bit stream (page 2, line 32 to page 3, line 8, and Figure 1; Chiariglione '98).

To incorporate the multiplexing in of variance information into the encrypted bit stream as taught by Chiariglione '98, to the Jones '730 / Nardone '700 / Leppek '501 combination, would have been obvious to a person having ordinary skill in the art at the time of the invention as the combination of the same is necessary and explicitly taught therein as will be demonstrated below.

The motivation to transmit dynamically varying encryption policy information via the Chiariglione '98 within the context of the Jones '730 / Nardone '700 / Leppek '501 combination is suggested by the fact that both disclosures are refer to the encryption/decryption of multimedia data. Selectively encrypt a bit stream as taught by Nardone '700 is a direct consequence of handling multimedia data. The Chiariglione '98 teaching discusses the MPEG-2 specification, which discloses use of EMM and ECM messages multiplexed into the bit stream in order to provide access control information dynamically. In order to take advantage of the MPEG market, the inventor would have been motivated to use of EMM and ECM messages multiplexed into the bit stream as taught by the MPEG specification. As such, it would have been necessary and obvious to apply the Chiariglione '98 teaching with the Jones '730 / Nardone '700 / Leppek '501 combination in order to be compliant with the MPEG specification and thus be salable in the MPEG market. Thus Claim 4 is rejected under 35 USC 103(a).

<u>Claim 21:</u>

Regarding Claim 21, Jones '730 teaches all the limitations of Claim 14. However, Jones '730 does not teach multiplexing in the encryption parameter in with the bit stream.

However, the Jones '730 / Nardone '700 / Leppek '501 / Chiariglione '98 combination described in the discussion regarding Claim 4 above teaches multiplexing in the encryption parameter in with the bit stream.

It would have been necessary and obvious for a person having ordinary skill in the art to modify Jones '730 to multiplex in the encryption parameter in with the bit stream as

described in the discussion above regarding Claim 4. Thus Claim 21 is rejected under 35 USC 103(a).

6. Claim 28 is rejected under 35 U.S.C. 103(a) as being anticipated by U.S. Patent No. 5,719,937 issued to Warren et al. (Warren '937), in view of Nardone '700, and in further view of Leppek '501.

Claim 28:

Regarding Claim 28, Warren '937 teaches corresponding limitations, specifically a program storage device readable by a machine, tangibly embodying at least one program of instructions executable by the machine to perform a method for protecting a stream of data to be transferred between an encryption unit and a decryption unit (column 3, lines 42-47; column 6; lines 28-36; Warren '937), comprising;

- encrypting the stream of data at said encryption unit for transfer thereof to said decryption unit (column 3, line 65 to column 4, line 13; Warren '937);
- dynamically varying said encrypting of said stream of data at said encryption unit by changing an encryption parameter and signaling said change in encryption parameter and signaling said change in encryption parameter to said decryption unit, wherein said dynamically varying of said encryption parameter is responsive to occurrence of a predefined condition in said stream of data (column 4, lines 6-12; Warren '937); and

- decrypting said encrypted data at the decryption unit, said decrypting accounting for said dynamic varying of said encrypting by said encryption unit using said changed encryption parameter (column 6, line 36 to column 7, line 45 ; Warren '937).

The preferred embodiment of Warren '937 is to embed tags that hold metadata that determine mode of encryption, and may be encoded in real-time (column 4, line 8; Warren '937). In the disclosed example, the tags can specify a number of ways to vary encryption in a bit stream (column 5, lines 28-36; Warren '937). Furthermore, the decryptor works in a complementary way. Finally, the data can be persisted in media such as a DVD or CD (column 6, lines 27-37; Warren '937) but may apply to any compatible storage media. Thus Warren '937 teaches all the limitations of Claim 28.

Furthermore, regarding Claim 28 as amended, Warren '937 teaches corresponding limitations as Jones '730. However, Warren '937 does not explicitly teach the additional limitations regarding "dynamically changing parameters simultaneously" and "multiple parameters."

Nardone '700 teaches dynamically changing encryption parameters as described in paragraphs 12-13 below. However, Nardone '700 does not explicitly teach setting multiple parameters.

Leppek '501 teaches setting multiple parameters as described in paragraphs 12-13 below.

It would have been obvious to a person having ordinary skill in the art to combine Warren '937, Nardone 700, and Leppek '501 on the same basis as described in

paragraphs 12-13 below wherein the Jones '730 reference is replaced with the Warren '937 reference.

7. Claims 29-30 and 32-38 are rejected under 35 U.S.C. 103(a) as being unpatentable in view of Jones '730 in view of Warren '937, and in further view of Nardone '700 and moreover in view of Leppek '501.

Claims 29 and 32-25 (as amended):

Regarding Claims 29 and 32-35, Jones '730 teaches corresponding limitations in all the aforementioned claims with the exception of explicitly teaching a program storage device. Refer to the discussions regarding Claims 2, and 5-8 respectively.

Warren '937 teaches a program storage device (column 6, lines 28-36; Warren '937) as described in the discussion regarding Claim 28 above.

The motivation to apply the encryption scheme of Jones '730 to the program storage device of Warren '937 is suggested by Warren '937, "it would be desirable to provide an electronic copy management scheme for controlling the reproduction of proprietary data" (column 1, lines 36-38; Warren '937). In fact, Warren '937 discloses one such invention. Furthermore, the motivation to use the method of Jones '730 is suggested by Jones '730, "For increased data security, the encryption key value may be changed frequently to further reduce the likelihood that an unauthorized party may decipher the data" (column 1, lines 22-25; Jones '730). Thus an implementer who used the program storage device and copy management method of Warren '937, who desired

to reduce the ability to hack the data would be motivated to add the encryption method of Jones '730.

Furthermore, regarding Claims 29 and 32-35 as amended Jones '730 does not explicitly teach the additional limitations regarding "dynamically changing parameters simultaneously" and "multiple parameters."

Nardone '700 teaches dynamically changing encryption parameters as described in paragraphs 12-13 below. However, Nardone '700 does not explicitly teach setting multiple parameters.

Leppek '501 teaches setting multiple parameters as described in paragraphs 12-13 below.

It would have been obvious to a person having ordinary skill in the art to combine Nardone 700 and Leppek '501 with Jones '730 and Warren '937 on the same basis as described in paragraphs 12-13 below.

<u>Claims 30 and 36-38 (as amended):</u>

Regarding Claims 30 and 36-38, Jones '730, Nardone '700, and Leppek '501 in combination teach corresponding limitations in all the aforementioned claims with the exception of explicitly teaching a program storage device. Refer to the discussions regarding Claims 3, 14, 10, and 11 respectively.

The motivation to apply the encryption scheme of the Jones '730 / Nardone '700 / Leppek '501 combination to the program storage device of Warren '937 is suggested by Warren '937, "it would be desirable to provide an electronic copy management scheme for controlling the reproduction of proprietary data" (column 1, lines 36-38; Warren

'937). In fact, Warren '937 discloses one such invention. Furthermore, the motivation to use the method of the Jones '730 / Nardone '700 / Leppek '501 combination is suggested by Warren '937, "it is assumed that the source material which is stored on the media is compressed data, and that the media is a laser disk, compact disk, or DVD" (column 6, lines 28-31; Warren '937). The context of the Warren '937 invention is that of multimedia data. As discussed above, the Jones '730 / Nardone '700 / Leppek '501 provides a cryptographic combination motivated to be applied to multimedia data. Thus a practitioner ordinarily skilled in the art would be motivated to apply the Jones '730 / Nardone '700 / Leppek '501 method to the program storage device of Warren '937. Thus Claims 30, and 36-38 are rejected under 35 USC 103(a).

Furthermore, regarding Claims 30 and 36-38 as amended note that Nardone '700 teaches dynamically changing encryption parameters and Leppek '501 teaches setting multiple parameters as described in paragraphs 12-13 below.

8. Claim 31 is rejected under 35 U.S.C. 103(a) as being unpatentable over Jones '730, Nardone '700, Leppek '501, and Chiariglione'98 in view of Warren '937.

Claim 31:

Regarding Claim 31, Jones '730, Nardone '700, Leppek '501, and Chiariglione'98 teach corresponding limitations with the exception of explicitly teaching a program storage device as described in the discussion regarding Claim 4 above.

Warren '937 teaches a program storage device (column 6, lines 28-36; Warren '937) as described in the discussion regarding Claim 28 above.

The motivation to apply the encryption scheme of the Jones '730 / Nardone '700 / Leppek '501 / Chiariglione '98 combination to the program storage device of Warren '937 is suggested by Warren '937, "it would be desirable to provide an electronic copy management scheme for controlling the reproduction of proprietary data" (column 1, lines 36-38; Warren '937). In fact, Warren '937 discloses one such invention. Furthermore, the motivation to use the method of the Jones '730 / Nardone '700 / Leppek '501 / Chiariglione '98 combination is suggested by Warren '937, "it is assumed that the source material which is stored on the media is compressed data, and that the media is a laser disk, compact disk, or DVD" (column 6, lines 28-31; Warren '937). The context of the Warren '937 invention is that of multimedia data. As discussed above, the Jones '730 / Nardone '700 / Leppek '501 / Chiariglione '98 provides a cryptographic combination, including multiplexing encryption data. Thus a practitioner with ordinary skill in the art would be motivated to apply the Jones '730 / Nardone '700 / Leppek '501 / Chiariglione '98 method to the program storage device of Warren '937.

(11) Response to Arguments

(11.1) Response to Group I Arguments

11.1A Jones '730 in combination with Nardone '700 and Leppek '501 in fact discloses "encrypting a stream of data and during the encryption process dynamically varying encrypting of the stream of data by dynamically changing simultaneously multiple encryption parameters." (Appeal Brief: p. 7, lns. 1-4).

Examiner points out that it is not enough to assert that Jones '730 does not disclose a claimed limitation. Rather, the Applicant must show that the combination of references does not disclose the claimed limitation. Jones '730, Nardone '700, and Leppek '501 in combination in fact disclose "encrypting a stream of data and during the encryption process dynamically varying encrypting of the stream of data by dynamically changing simultaneously multiple encryption parameters", as quoted from paragraph 12 of the Final Office Action:

- Encryption devices send encrypted data to decryption devices. It is well known in the art to vary the means of encryption in an encryption device in order to improve security [Examiner Note – Final Office action did not disclose that this assertion was taught by Jones '730, col. 1, lns. 22-24]. Jones '730 teaches one such invention wherein an encryption device whose means of encryption involves an encryption key and whose means of varying encryption is by varying the encryption key (Jones '730: col. 1, lns. 22-35). While varying the encryption key is one was to vary the means of encryption, it is not the only way to vary the means of encryption. The insight of Jones '730 is in the varying of the means of encryption.
- Dynamically changing encryption parameters used to encrypt the stream of data is a valid way to vary the means of encryption. Nardone '700 teaches specifying encryption parameters via a policy (i.e. the degree of selective encryption in order to degrade video image) (Nardone '700: col. 1, lns. 40-50). Furthermore, Nardone '700 teaches the dynamic changing of encryption policies (Nardone '700: col. 1, lns. 51-59). Since a policy teaches the setting of encryption parameters and dynamic changing of encryption policies reads on dynamic changing of encryption parameters. While varying the degree of selective encryption in order to degrade video image is one possible encryption parameter to vary, it is not the only encryption parameter to vary. The insight of Nardone '700 is the use of policies that specify parameters to vary and the dynamic changing simultaneously multiple encryption parameters via dynamically changing policies.
- Where Nardone '700 is not explicit about setting multiple parameters in a policy, Leppek '501 is explicit about setting multiple encryption parameters. Leppek '501 teaches applying multiple encryption operators (Leppek '501: col. 1, ln. 64 to col. 2, ln. 5). Encapsulating the setting of multiple encryption parameters of Leppek '501 into a single policy of

Nardone '700, and having a multiplicity of different policies (i.e. different multiple encryption parameters set), and dynamically changing policies as taught by Nardone '700 (supra), fully reads on dynamically changing simultaneous multiple encryption parameters. The insight of Leppek '501 is the application of multiple encryption operators at once.

- The motivation to combine Nardone '700 with Jones '730 is suggested by Nardone '700, i.e. the policies of Nardone '700 teach partial encryption in order to save processing cycles on encrypting data. Applying the policies of Nardone '700 to Jones '730 creates a combination in which enables selective encryption of the bit stream to save cycles and provide fast encryption of streaming data (Nardone '700: col. 1, lns. 45-50). The insight of this combination is rather than Jones '730 simply changing encryption keys, Jones '730 can change policies as per Nardone '700 where each policy contains an independent setting of encryption parameters.
- The motivation to apply the multiple parameters of Leppek '501 with the Nardone '700 and Jones '730 combination, i.e. to have each of a plurality of policies of Nardone '700 specify multiple parameters, and further to have said plurality of policies be dynamically changed, is suggested by Leppek '501 which states that varying encryption schemes reduces cryptographic footprint and thus increases security (Leppek '501: col. 1, lns. 54-60; col. 1, lns. 65-67). This is analogous to the teaching of Jones '730 which states that changing an encryption parameter increases data security (Jones '730: col. 1, lns. 15-21). The insight of applying Leppek '501 to the Nardone '700 and Jones '730 combination is that Jones '730 can change policies as per Nardone '700 where each policy contains an independent setting of a multiplicity of encryption parameters.

11.1B Jones '730 in combination with Nardone '700 and Leppek '501 in fact discloses "signaling the dynamic change in the encryption parameters <u>from the encryption unit to the decryption unit." (Appeal Brief: p. 7, lns. 15-16).</u>

Examiner points out that it is not enough to assert that Jones '730 does not disclose a claimed limitation. Rather, the Applicant must show that the combination of references does not disclose the claimed limitation. Jones '730, Nardone '700, and Leppek '501 in combination in fact disclose "signaling the dynamic change in the encryption parameters

from the encryption unit to the decryption unit", as quoted from paragraph 12 of the Final Office Action:

- The Jones '730 patent, still requires the exchange of random number seed values and interval values between the encryptor and decryptor (Jones '730: col. 1, ln. 66 to col. 2, ln. 7). The exchange of random number seed values and/or interval values constitutes and event that causes a change in encryption by encryptor and decryptor.
- Within the context of the Jones '730, Nardone '700, and Leppek '501 combination,
- On this basis, the Jones '730, Nardone '700, and Leppek '501 combination reads on "signaling the dynamic change in the encryption parameters from the encryption unit to the decryption unit.

11.1C Examiner does not mischaracterize Jones '730, in stating that there is no, "dynamic signaling of information <u>per se from the encryption unit to the decryption unit." (Appeal Brief: p. 8, lns. 1-3).</u>

Applicant attempts to distinguish itself from Jones '730 which relies on block counters to detect changes (Jones '730: Fig. 1), where pending application relies on multiplexing parameter changes. However, Examiner points out that independent claims 1 and 14 as currently written do not reflect this limitation. In fact, Claim 4, which is not in Group I, is the claim that includes a multiplexing limitation, and is addressed under Group III.

Claim 1 reads in part:

> dynamically varying of said multiple encryption parameter being responsive to occurrence of a predefined condition in said stream of data (Appeal Brief: p. 16, lns. 9-10)

The term dynamically varying reads on *any* change of encryption parameter caused by a predefined condition. Jones '730 changes an encryption key which reads on an

encryption parameter (Jones '730: col. 1, lns. 22-35). Futhermore, the term, "predefined condition", reads on *any* condition in the stream of data. This includes a predetermined number of blocks of the data stream passing. In fact Applicant's Claim 5 (part of Group I) specifically claims, "based on passage of a predetermined number of units of physical data or passage of a predefined number of conceptual units of data" (Appeal Brief: p. 15, lns. 24-25). Since the block counters of Jones '730 rely on a predetermined number of blocks in the data stream passing (Jones '730: col. 12, lns. 35-37; col. 12, lns. 48-49; col. 3, lns. 33-36; col. 3, lns. 64-68), Jones '730, Nardone 700, and Leppek '501 read on Applicant's claims.

11.1D Leppek '501 in combination with Jones '730 and Nardone '700 in fact disclose applying multiple encryption operators to the same data rather than applying multiple encryption operators to a stream of data <u>as it passes as claimed in the pending application (Appeal Brief: p. 10, lns. 8-12).</u>

Examiner points out that it is not enough to assert that Leppek '501 does not disclose a claimed limitation. Rather, the Applicant must show that the combination of references does not disclose the claimed limitation. Jones '730, Nardone '700, and Leppek '501 in combination in fact disclose applying multiple encryption parameters to a stream of data. Examiner reiterates counterargument to Applicant's argument 11.1A (supra) that Jones '730 discloses varying of encryption means to a stream of data, further that Nardone '700 discloses varying encryption parameters, and that Leppek '501 discloses setting multiple encryption parameters. The combination of Jones '730, Nardone '700, and Leppek '501, thus has Leppek '501 applied to a stream of data.

11.1E A person having ordinary skill in the art is in fact motivated to combine Jones '730, Nardone '700, and Leppek '501 (Appeal Brief: p. 10, lns. 13-14, p. 10, lns. 23-25).

Examiner points out that the person having ordinary skill in the art is a cryptographer who would be familiar with the encryption schemes of Jones '730, Nardone '700, and Leppek '501. Such a person faced with the problem of increasing the security of a data stream would naturally have been drawn to changing encryption parameters as disclosed by the combination (Leppek '501: col. 1, lns. 54-60; col. 1, lns. 65-6; Jones '730: col. 1, lns. 15-21).

Examiner reiterates counterargument to Applicant's argument 11.1A (supra) which discusses motivation to combine.

Examiner further points out that Jones '730, Nardone '700, and Leppek '501 in combination in fact disclose "a mechanism for signaling dynamic changes in multiple parameters." Examiner reiterates counterargument to Applicant's argument 11.1C (supra) which discusses the block count of Jones '730 reading on signaling dynamic changes.

Examiner reiterates counterargument to Applicant's argument 11.1C (supra) that independent claims 1 and 14 as currently written do not reflect a mechanism to signal dynamic changes and that Claim 4, which is not in Group I, is the claim that includes a multiplexing limitation, and is addressed under Group III.

(11.2) Response to Group II Arguments

11.2A Examiner reiterates counterarguments 11.1A through 11.1E as applied to Aucsmith '403 (Appeal Brief: p. 11, lns. 11-14).

Examiner reiterates counterarguments to Applicant reiterated arguments 11.1A through 11.1E.

Examiner opts to expand on how Aucsmith '403 is structurally analogous to Jones '730. Where Jones '730 relies on a block counter to count blocks in a data stream before changing encryption parameters, Aucsmith '403 counts Groups of Pictures (GOPs) (Aucsmith '403: col. 2, lns. 28-30).

(11.3) Response to Group III Arguments

11.3A Chiariglione '98 combined with Jones '730, Nardone '700, and Leppek '501, in fact discloses "dynamic changes of the multiple parameters from an encryption unit to a decryption unit by multiplexing the changed encryption parameters themselves with the encrypted data" (Appeal Brief: p. 12, lns. 11-18).

Examiner points out that it is not enough to assert that Chiariglione '98 does not disclose a claimed limitation. Rather, the Applicant must show that the combination of references does not disclose the claimed limitation. Since Chiariglione '98 discloses multiplexing parameters into a data stream (Chiariglione '98: p. 2, ln. 32 to p. 3, ln. 8, and Fig. 1),

combined with Jones '730, Nardone '700, and Leppek '501, in fact discloses "signaling ... dynamic changes of the multiple parameters from an encryption unit to a decryption unit by multiplexing the changed encryption parameters themselves with the encrypted data."

Examiner quotes the motivation to combine Chiariglione '98 to Jones '730, Nardone '700, and Leppek '501 from the rejection of Claim 4 in paragraph 6 of the Final Office Action:

> To incorporate the multiplexing in of variance information into the encrypted bit stream as taught by Chiariglione '98, to the Jones '730 / Nardone '700 / Leppek '501 combination, would have been obvious to a person having ordinary skill in the art at the time of the invention as the combination of the same is necessary and explicitly taught therein as will be demonstrated below.
>
> The motivation to transmit dynamically varying encryption policy information via the Chiariglione '98 within the context of the Jones '730 / Nardone '700 / Leppek '501 combination is suggested by the fact that both disclosures are refer to the encryption/decryption of multimedia data. Selectively encrypt a bit stream as taught by Nardone '700 is a direct consequence of handling multimedia data. The Chiariglione '98 teaching discusses the MPEG-2 specification, which discloses use of EMM and ECM messages multiplexed into the bit stream in order to provide access control information dynamically. In order to take advantage of the MPEG market, the inventor would have been motivated to use of EMM and ECM messages multiplexed into the bit stream as taught by the MPEG specification. As such, it would have been necessary and obvious to apply the Chiariglione '98 teaching with the Jones '730 / Nardone '700 / Leppek '501 combination in order to be compliant with the MPEG specification and thus be salable in the MPEG market. Thus Claim 4 is rejected under 35 USC 103(a).

(11.4) Response to Group IV Arguments

11.4A Examiner reiterates counterarguments to Applicant's reiterated arguments
11.1A through 11.1E regarding the Group IV claims (Appeal Brief: p. 13, lns. 1-13).

Examiner reiterates counterarguments to Applicant reiterated arguments 11.1A through 11.1E (supra).

(11.5) Response to Group V Arguments

11.5A Examiner reiterates counterarguments to Applicant's reiterated arguments 11.1A through 11.1E regarding the Group V claims (Appeal Brief: p. 13, ln. 18 to p. 14, ln. 3).

Examiner reiterates counterarguments to Applicant arguments 11.1A through 11.1E (supra).

(11.6) Response to Group VI Arguments

11.6A Examiner reiterates counterarguments to Applicant's reiterated arguments
11.1A through 11.1E regarding the Group VI claims (Appeal Brief: p. 14, lns. 8-18).

Examiner reiterates counterarguments to Applicant arguments 11.1A through 11.1E (supra).

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Patrick J.D. Santos
December 7, 2004

Conferees
Safet Metjahic, John Breene

KEVIN P RADIGAN ESQ
HESLIN & ROTHENBERG PC
5 COLUMBIA CIRCLE
ALBANY, NY 12203-5160

Safet Metjahic

SAFET METJAHIC
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

John E. Breene

JOHN BREENE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100